

PTH:CWE
F. #2021R00301

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
SAMSUNG GALAXY PHONE SM-S111DL,
GALAXY A01, ANDROID ID
6ea2a71f4b9cd023, THAT IS STORED AT A
PREMISES CONTROLLED BY UNITED
STATES PROBATION

**AGENT AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH AND
SEIZURE WARRANT**

Case No. 21 MJ 655

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, DAVID EIDAM, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Department of Labor - Office of Inspector General (“DOL-OIG”) Special Agent since March 2017. As such, I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I am currently assigned to DOL-OIG’s New York Region and I am a task force agent with the United States Department of Homeland Security, Homeland Security Investigations (“HSI”) in New York, NY. My duties as a Special Agent are to investigate labor racketeering and criminal violations within the programs of the United States Department of Labor. I have experience in interviewing, interrogation techniques, surveillance, financial crimes, identity theft, computer-related crimes, and the execution of search warrants of electronic data and devices.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the electronically stored information

specified below (the “Subject ESI”) for the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience, and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information (“ESI”). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

3. The Subject ESI is particularly described as all content and other information associated with electronic data imaged from the Samsung Galaxy phone SM-S111DL, Galaxy A01, Android ID 6ea2a71f4b9cd023 (the “SUBJECT PHONE”), pursuant to United States Probation’s consent on or about April 27, 2021, and maintained at premises controlled by the United States Probation at 202 Federal Plaza, Central Islip, New York 11722.

4. Based on my training, experience, and research, and as described below, I know that the SUBJECT PHONE has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA.

5. The Subject ESI is presently located in the Eastern District of New York.

THE SUBJECT OFFENSES

6. For the reasons detailed below, I believe that there is probable cause to believe that the SUBJECT PHONE contains evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 641 (theft of government funds), 1028A (aggravated identity

theft), 1029 (access devise fraud), 1343 (wire fraud), and 1341 (mail fraud) (collectively, the “Subject Offenses”).

PROBABLE CAUSE

7. I have been involved in an investigation into TROY JONES, an individual who is being monitored on supervised release by United States Probation out of the Eastern District of New York. The investigation is being conducted by DOL-OIG, the New York State Department of Labor (“NYSDOL”), and United States Probation.

8. Based on my participation in this investigation and my conversations with other law enforcement agents, including investigators from NYSDOL, I have learned the following, in substance and in part.

I. Background Regarding Unemployment Insurance Fraud Schemes

9. Unemployment Insurance (“UI”) is a state-federal program that provides monetary benefits to eligible lawful workers. Although state workforce agencies (SWAs) administer their respective UI programs, they must do so in accordance with federal laws and regulations. UI payments (benefits) are intended to provide temporary financial assistance to lawful workers who are unemployed through no fault of their own. Each state sets its own additional requirements for eligibility, benefit amounts, and length of time benefits can be paid. Generally, UI weekly benefit amounts are based on a percentage of your earnings over a base period. In the State of New York, the NYSDOL administers the UI program.

10. On March 13, 2020, the President declared the ongoing Coronavirus Disease 2019 (“COVID-19”) pandemic of sufficient severity and magnitude to warrant an emergency declaration for all states, tribes, territories, and the District of Columbia pursuant to section 501

(b) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. Sections 5121-5207 (the “Stafford Act”).

11. On March 18, 2020, the President signed the Families First Coronavirus Response Act (“FFCRA”) into law. The FFCRA provides additional flexibility for state UI agencies and additional administrative funding to respond to the COVID-19 pandemic. The Coronavirus Aid, Relief, and Economic Security (“CARES”) Act was signed into law on March 27, 2020. It expands states’ ability to provide UI for many workers impacted by COVID-19, including for workers who are not ordinarily eligible for UI benefits. The CARES Act provided for three new UI programs: Pandemic Unemployment Assistance (“PUA”); Federal Pandemic Unemployment Compensation (“FPUC”); and Pandemic Emergency Unemployment Compensation (“PEUC”).

12. The first program, PUA, provides for up to 39 weeks of benefits to individuals who are self-employed, seeking part-time employment, or otherwise would not qualify for regular UI or extended benefits under state or federal law or PEUC under section 2107 of the CARES Act. Coverage includes individuals who have exhausted all rights to regular UC or extended benefits under state or federal law or PEUC. Under the PUA provisions of the CARES Act, a person who is a business owner, self-employed worker, independent contractor, or gig worker can qualify for PUA benefits administered by NYSDOL if he/she previously performed such work in New York and is unemployed, partially unemployed, unable to work, or unavailable to work due to a COVID-19 related reason. A PUA claimant must answer various questions to establish his/her eligibility for PUA benefits. The claimant must provide his/her name, Social Security Number, and mailing address. The claimant must also identify a qualifying occupational status and COVID-19 related reason for being out of work. The eligible

timeframe to receive PUA is from weeks of unemployment beginning on or after January 27, 2020 through December 31, 2020.

13. The second program, PEUC, provides for up to 13 weeks of benefits to individuals who have exhausted regular UI under state or federal law, have no rights to regular UI under any other state or federal law, are not receiving UI under the UI laws of Canada, and are able to work, available for work, and actively seeking work. However, states must offer flexibility in meeting the “actively seeking work” requirement if individuals are unable to search for work because of COVID-19, including because of illness, quarantine, or movement restriction. The eligible timeframe to receive PEUC is from weeks of unemployment beginning after the respective state has an established agreement with the federal government -- the earliest being April 5, 2020 -- through December 31, 2020.

14. The third program, FPUC, provides individuals who are collecting regular UI, PEUC, PUA, and several other forms of UC with an additional \$600 per week. The eligible timeframe to receive PEUC was from weeks of unemployment beginning after the respective state had an established agreement with the federal government -- the earliest being April 5, 2020 -- through July 31, 2020.

15. On August 8, 2020, after FPUC expired, the President signed a Presidential Memorandum authorizing FEMA to use disaster relief funds pursuant to Section 408 Other Needs Assistance of the Stafford Act to provide supplemental payments for lost wages to help ease the financial burden on individuals who were unemployed as a result of COVID-19. The “Lost Wages Assistance Program” (“LWAP”) served as a temporary measure to provide an additional \$300 per week via a total of \$44 billion in FEMA funds. The period of assistance for

LWAP is August 1, 2020 to December 27, 2020, or termination of the program, whichever is sooner.

16. In total, more than \$300 billion in additional federal funds for UI have been appropriated in 2020.

17. The NYSDOL offers an online website (“the Website”) through which applicants can apply for the above and other benefits. To apply for benefits through the Website, an applicant must complete a form that includes, among other things, the applicant’s name, date of birth, social security number, and address. Moreover, NYSDOL sometimes requires additional documents, including photo identification. In addition, the applicant can direct that the NYSDOL send any approved funds to a specific bank account or to a debit card. The debit cards are issued from KeyBank (“KeyBank Cards”). Before NYSDOL issues funds, NYSDOL verifies that, among other things, the applicant, based on his or her social security number, has worked in New York and is eligible for benefits.

18. Based upon a review of internal records from the NYSDOL, the State of New York has advised that many claims made pursuant to the above-described programs are fraudulent. Based on my training and experience, and the investigation to date, I am aware that numerous fraudulent claims have been made in 2020 and 2021 for the purpose of obtaining Unemployment Insurance Benefits (“UIBs”) from the State of New York as well as numerous other States. The resulting losses are at least in the hundreds of millions of dollars.

II. Seizure of the SUBJECT PHONE

19. On November 25, 2020, TROY JONES commenced supervised release in the Eastern District of New York. Pursuant to the terms of his supervised release, TROY JONES was required to comply with special conditions including, but not limited to, a search condition and the Computer and Internet Monitoring Program (“CIMP”).

20. The CIMP required, among other things, that “[a]ny computer and/or other device which allows Internet access and/or digital media storage within [TROY JONES’s] residence, or otherwise accessible by [TROY JONES], is subject to random examinations/analysis/search by [United States Probation].”

21. The terms of TROY JONES’s supervised release also restricted his access to computers and other devices such as mobile telephones. Accordingly, he was only permitted to have access to mobile telephone devices that were both authorized and monitored by United States Probation.

22. Additionally, with respect to his probation officer, the terms of TROY JONES’s supervised release stated that he, “must allow the probation officer to visit [him] at any time at [his] home or elsewhere, and [he] must permit the probation officer to take any items prohibited by the conditions of [his] supervision that he or she observes in plain view.”

23. On or about February 25, 2021, United States Probation officers conducted a home visit with TROY JONES. During the home visit, a United States Probation officer observed a bulge inside of TROY JONES’s pants pocket, that appeared to look like a phone because of its shape and size. After a United States Probation officer inquired about the item in TROY JONES’s pocket, TROY JONES removed it from his pocket. It was a Samsung Galaxy phone SM-S111DL, Galaxy A01, Android ID 6ea2a71f4b9cd023, the SUBJECT PHONE. In response to a request, TROY JONES handed the SUBJECT PHONE to one of the United States Probation officers. TROY JONES had not been authorized by United States Probation to have access to the SUBJECT PHONE, and it had not been monitored.

24. The SUBJECT PHONE was seized by United States Probation officers. The United States Probation officers later explained to me that they had the authority to seize and search the SUBJECT PHONE pursuant to the terms of TROY JONES's supervised release.

25. Later, United States Probation officers conducted a review of the content on the SUBJECT PHONE. Their review included viewing images, messages, and other applications on the SUBJECT PHONE.

26. During United States Probation officers' search of the SUBJECT PHONE, United States Probation officers found messages on the SUBJECT PHONE suggesting that TROY JONES had used the SUBJECT PHONE to communicate with other individuals. For example, the messages in sum and substance asserted that they were coming from TROY JONES.

27. During their review of the content on the SUBJECT PHONE, United States Probation officers found personal identifying information for ten individuals and certain images of online applications for unemployment insurance benefits. TROY JONES's United States Probation officer told me that the individuals whose personal information was found on the SUBJECT PHONE did not appear to have any connection to TROY JONES.

28. A United States Probation officer reached out to NYSDOL and DOL-OIG and provided the information that was found on the SUBJECT PHONE. The NYSDOL and DOL-OIG used the information that the United States Probation officer provided to determine whether there were any UI claims made on behalf of the individuals whose personal identifying information was on SUBJECT PHONE and, if so, whether there were any red-flags associated with the claims. The NYSDOL also conducted a search of information related to TROY JONES's application for unemployment insurance benefits.

III. Probable Cause to Believe Evidence of Crimes is Contained on the SUBJECT PHONE¹

29. TROY JONES filed his personal UI claims from a particular IP address (the “IP Address”).

30. On or about and between June 11, 2020 and January 29, 2021, both dates being approximate and inclusive, the status of approximately 45 claims (the “45 Claims”) were checked from the IP Address. The 45 Claims included those for the ten individuals of whom personal identifying information was found on the SUBJECT PHONE by United States Probation officers. The IP Address was a “static” IP address during the relevant time period. Based upon my training and experience, a static IP address is an address that is assigned to one and only one subscriber.

31. On or about and between March 9, 2020, and November 30, 2020, both dates being approximate and inclusive, the 45 Claims were submitted to the Website.

32. The 45 Claims were submitted using names and personal identifying information of real individuals, many of whom were from different states. The personal identifying information in the 45 Claims included: names, dates of birth, social security numbers, and driver’s license numbers. Most of the claims were for PUA self-employment benefits.

33. For example, Victim-1’s UI claim was submitted from the IP Address. Victim-1 was an individual whose personal identifying information was found on the SUBJECT PHONE

¹ Because TROY JONES is on supervised release and subject to conditions overseen by United States Probation that reduce his expectation of privacy with respect to certain devices that he has access to, and the device is now in the possession, custody, and control of United States Probation pursuant to the authority they represented to have under the terms of TROY JONES’s supervised release, the Government does not believe that a warrant or probable cause is technically required in order to search and seize the SUBJECT ESI. However, out of an abundance of caution, the Government is seeking the current search and seizure warrant.

by the United States Probation officers. The personal identifying information that was contained on the SUBJECT PHONE belonging to Victim-1 included his date of birth, New York State driver's license number, home address, email, and username for the Website.

34. According to NSYDOL records, Victim-1's home address is in Westchester County, NY but the "home" address for which he registered to receive benefits was in Nassau County, New York.

35. Based upon the foregoing, I believe that Victim-1's claim was fraudulent.

36. Similarly, Victim-2's UI claim was submitted from the IP Address. However, upon a search of Victim-2's social security number in law enforcement databases, I have discovered that Victim-2 lives, works, and files taxes in Glendale, Arizona. Victim-2 would not be eligible to receive UIBs from the NYSDOL and is therefore not likely to have filed for UIBs in New York from the IP Address.

37. Based upon the foregoing, I also believe that Victim-2's claim was fraudulent.

38. Based on my review of NYSDOL records relating to the 45 Claims, I have learned that many of the 45 Claims requested that any approved funds be deposited into KeyBank Cards.

39. Further, upon a review of NYSDOL records related to the 45 claims, I have learned that many of the KeyBank Cards have been sent to either TROY JONES's address or other addresses rather than to the home addresses corresponding with the individuals on whose behalf the UIBs were requested.

40. Based on my training and experience and my participation in this investigation, I know that individuals who receive UI funds on KeyBank Cards often visit ATMs to withdraw cash on those cards.

41. I believe that a majority (if not all) of the 45 Claims describe above were fraudulent based on the following facts: (i) the 45 Claims were submitted using names and personal identifying information of real individuals, many of whom are from outside of New York state, but they all listed TROY JONES's address or other addresses rather than the individuals' own addresses as the location to receive benefits; (ii) TROY JONES's United States Probation officer indicated a lack of any connection between TROY JONES and the individuals on whose behalf the 45 claims were made, much less a connection relating to the filing for unemployment insurance benefits (which would be a violation of the terms of TROY JONES's supervision); and (iii) the status of the 45 Claims were checked for New York UI claims using the IP Address despite the fact that some of the individuals live and work outside of New York.

42. Based on my review of reports and my conversations with other agents involved in the investigation and United States Probation, our preliminary investigation has revealed that the files uncovered on the SUBJECT PHONE include evidence of fraudulent Unemployment Insurance and CARES Act claims totaling approximately \$200,000.

43. Based on my training and experience and my participation in this investigation, I know that, in order to file or check on the status of UIBs claims, a user must use an electronic device, such as a cellphone or computer. Further, I know that, when individuals file for or check on the status of UIBs, they require access to documents containing personal identifying information so that they can complete their application, submit necessary supporting documents along with their application, or log in to check the status of their claim. Thus, people who file fraudulent claims for UIBs require access to such documents and personal identifying information of other people in order to submit fraudulent claims on behalf of others. I also know that such individuals frequently store those documents and personal identifying information on electronic

devices in order to, among other things, keep a record of fraudulent claims for future reference; keep an accounting of illegal proceeds; and store false or stolen data for future exploitation.

44. Further, individuals who file fraudulent UIBs frequently rely on cellphone communications to communicate with other co-conspirators regarding victims of the scheme. Such persons also commonly maintain contact information relating to their criminal associates – including names, telephone numbers, direct connect numbers, and/or addresses – and store records relating to their illegal activity on electronic devices. Such records can include, for example, logs of online “chats” with co-conspirators; email correspondence; contact information of co- conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts; the personal identification data of victims, including names, addresses, telephone numbers, and social security numbers of other individuals; and/or records of fraudulent claims using false or stolen financial and personal identification data.

45. Accordingly, I respectfully submit there is probable cause to believe that TROY JONES engaged in, either directly or in concert with other unknown co-conspirators, the Subject Offenses, and that the following evidence of the Subject Offenses are likely to be found in the Subject ESI:

a. Evidence of the location of the owner(s) or user(s) of the Subject ESI, and co-conspirators and victims of the Subject Offenses;

b. Evidence concerning a fraudulent scheme to file applications for government funds and/or benefits, including (i) communications and information containing the personal identifying information of potential victims, (ii) communications or information concerning the application for or receipt of federal or state funds, including unemployment insurance benefits, (iii) communications or information concerning financial, bank, or other

account information used in furtherance of the Subject Offenses, and (iv) account information, including login credentials, relating to bank accounts, payment for identification information, or items used in furtherance of the Subject Offenses;

c. Evidence concerning the identity, location, or involvement in the Subject Offenses of TROY JONES and other co-conspirators;

d. Evidence concerning the identity of co-conspirators and victims in connection with the Subject Offenses, and communications with co-conspirators or others regarding the Subject Offenses;

e. Evidence concerning the use of the names and identities of others in furtherance of the Subject Offenses, including, but not limited to, the use of the names and identities of others to apply for government benefits;

f. Evidence, including documents, spreadsheets and ledgers, identifying and/or tracking victims, co-conspirators, fraudulent funds, and accounts used to receive, transfer, or launder fraudulent proceeds; and

g. Evidence concerning any online accounts or any electronic devices where evidence falling within the foregoing categories could be stored, including any passwords or encryption keys needed to access such evidence.

PROCEDURES FOR SEARCHING ESI

I. Review of ESI

46. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the SUBJECT ESI contained on the SUBJECT PHONE for information responsive to the warrant.

47. In conducting this review, law enforcement may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- a. surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- b. conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- c. “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and
- d. performing electronic keyword searches through all electronic storage areas to determine the existence and location of search terms related to the subject matter of the investigation. (Keyword searches alone are typically inadequate to detect all information subject to seizure. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.)

48. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement may need to conduct a complete review of all the ESI from the SUBJECT PHONE to locate all data responsive to the warrant.

49. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

II. Return of the Subject Device

50. If the Government determines that the SUBJECT PHONE is no longer necessary to retrieve and preserve the data on the device, and that the SUBJECT PHONE is not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return the SUBJECT PHONE to United States Probation. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) otherwise unlawfully possessed, or (iv) evidence of the Subject Offenses.

TECHNICAL TERMS

51. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and

e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS

navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from

and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

52. Based on my training, experience, and research, I know that SUBJECT PHONE has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

CONCLUSION

53. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

David Eidam

DAVID EIDAM
Special Agent
U.S. Department of Labor – Office of Inspector
General

Sworn to me through the transmission of this
Affidavit by reliable electronic means, pursuant to
Federal Rules of Criminal Procedure 41(d)(3) and 4.1, this
4th of June, 2021

/s Roanne L. Mann

HONORABLE ROANNE L. MANN
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

Attachment A

Device Subject to Search and Seizure

The electronically stored information (“ESI”) to be searched is described as electronic data imaged from a Samsung Galaxy SM-S111DL Galaxy A01, Android ID 6ea2a71f4b9cd023, pursuant to United States Probation’s consent on or about April 27, 2021, and maintained at premises controlled by the United States Probation at 202 Federal Plaza, Central Islip, New York 11722.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

Attachment B

Review of ESI on the Subject Device

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained on the Subject Device for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 641 (theft of government funds), 1028A (aggravated identity theft), 1029 (access devise fraud), 1343 (wire fraud), and 1341 (mail fraud) (the “Subject Offenses”) from January 1, 2020 to the present, described as follows:

- a. Evidence of the location of the owner(s) or use of the Subject ESI, and co-conspirators and victims of the Subject Offenses;
- b. Evidence concerning a fraudulent scheme to file applications for government funds and/or benefits, including (i) communications and information containing the personal identifying information of potential victims, (ii) communications or information concerning the application for or receipt of federal or state funds, including unemployment insurance benefits, (iii) communications or information concerning financial, bank, or other account information used in furtherance of the Subject Offenses, and (iv) account information, including login credentials, relating to bank accounts, payment for identification information, or items used in furtherance of the Subject Offenses;
- c. Evidence concerning the identity, location, or involvement in the Subject Offenses of TROY JONES and other co-conspirators;

d. Evidence concerning the identity of co-conspirators and victims in connection with the Subject Offenses, and communications with co-conspirators or others regarding the Subject Offenses;

e. Evidence concerning the use of the names and identities of others in furtherance of the Subject Offenses, including, but not limited to, the use of the names and identities of others to apply for government benefits;

f. Evidence, including documents, spreadsheets and ledgers, identifying and/or tracking victims, co-conspirators, fraudulent funds, and accounts used to receive, transfer, or launder fraudulent proceeds; and

g. Evidence concerning any online accounts or any electronic devices where evidence falling within the foregoing categories could be stored, including any passwords or encryption keys needed to access such evidence.